Data security & privacy

Information security

Like all organisations, the scale and complexity of cyber-attacks against the business continues to increase and we continue to identify, monitor and mitigate the risk this presents. During 2020, we moved over 8,500 colleagues to work from home as part of the business continuity response to the global pandemic which included the expansion of existing remote access services and investments in security tools and technology specifically to enhance security for home workers.

We continue to invest in IT security ensuring that the security posture of systems and services is maintained at an appropriate level, and continually monitored and improved.

Penetration testing exercises were undertaken to test our detection and response capability.

An information security awareness programme is helping to reduce security incidents and improve awareness. In 2020, this included phishing simulation exercises (involving over 15,000 colleagues in critical user functions with over 57,000 simulation emails sent in a series of campaigns), workshops and online training packages. Improvements to our email security capability were also implemented to enable users to identify high risk emails and improve technical resilience to phishing attacks. We also monitor external ratings using the Assessment of Business Cyber Risk framework provided by the US Chamber of Commerce and benchmark our cyber security where possible. We assess our performance against the National Institute of Standards and Technology (NIST) and align our policy framework and processes with ISO 27001 for information security. We want to do the right thing to ensure that our business and our customers can operate securely and safely.

Data protection

Rentokil Initial has implemented a Group Global Data Protection Policy that underpins its approach to data protection. This states the principles all businesses globally are expected to apply in data processing operational controls. The business globally requires use of a data protection tool provided by Onetrust to manage records of data processing, privacy impact assessments, data subject rights, consent management, cookie management and breach management.

Our global approach to data protection is aligned with the principles of the EU General Data Protection Regulation namely:

Lawfulness, fairness and transparency

As a global business we endeavour to ensure that personal data is processed lawfully, fairly and in a transparent manner that takes into account the rights of individuals as ‘data subjects’, whose personal data we process whether customers, employees or any others. We provide all individuals / data subjects with access to notices in multiple languages to provide transparency about how we manage personal data.

Purpose limitation

As part of our global compliance programme, we require all businesses to complete records of their processing activities. This requires process owners to have identified a specific purpose for processing that should be communicated in any privacy notices – public ones directed at customers, potential customers, suppliers, etc and those directed at potential employees / existing employees. Where any records of processing are created, we require an applicable lawful basis for processing, e.g. consent, contract or as otherwise applicable. For the purposes of transparency we have created records for over 75% of the countries we operate in globally and there is ongoing work to complete this data inventory exercise. We currently hold over 2,000 records of processing activities and anticipate that this may increase to 3,000 as the programme develops and matures.

Data minimisation

We have a network of over 100 local privacy officers / champions globally who supplement our dedicated expert resources and are encouraged to review the personal data processed to ensure we don’t process unnecessary data.

Accuracy

As a business we recognise that data has limited value if it is inaccurate and not updated. Improvements to our data quality are under regular review.

Storage limitation

We have a Document and Data Retention Policy which provides clarity on data retention and deletion requirements. Steps are being taken to improve compliance in this area globally in recognition of its importance as a compliance requirement.

Security, integrity and confidentiality

Our Global Data Protection Policy highlights the importance of applying appropriate security measures and ensuring any third parties we use to process personal data on our behalf apply appropriate security measures.

Data subject rights and access requests

We are able to manage data subject to requests for access, deletion, ‘do not sell data’, etc via our Onetrust privacy compliance tool and have effectively responded to all the requests received by the privacy team.

Transfers and data sharing

Any overseas transfers of personal data within group companies is subject to contractual arrangements based on EU approved Standard Model Clauses. We seek to include appropriate contract terms and controls based on assessments of EU / UK adequacy conditions or otherwise.

Data breach reporting

We have data breach notification guidelines that require attention and escalation at the earliest opportunity to the privacy team. Breaches can be reported directly to the team, via a self-service tool on the business intranet or via the IT reporting route. It is recognised that measures are required to raise awareness globally of breach management as knowledge / understanding in certain countries is in need of improvement.

Training and audit

Data protection training has been made available in 38 different languages to all staff. Completion rates do still vary somewhat but this is being pushed to improve engagement. The data protection programme is being reviewed globally by the internal audit team based on the Company’s core principles as aligned with the EU General Data Protection Regulation, and data protection forms part of internal audit reviews of operational business and functional teams (especially HR, marketing and IT).

Our privacy process lifecycle

We have an ongoing privacy process lifecycle as follows:

- Privacy Impact Assessments
- Creation of Records of Processing – which may require additional Data Protection Impact Assessments and Legitimate Interest Assessments
- Review of Records – ensure appropriate ownership, check details, validate lawful basis, identify risks and provide risk mitigation guidance
- Annual review and maintenance of records
- Review of privacy notices based on updates / changes to processing activities

It must be noted that we are at different stages of maturity and implementation of governance in the countries we operate in. Our baseline is to have a data inventory for all countries, to ensure most employees have completed training and have acknowledged applicable local employee privacy notices. Public facing privacy notices are available globally to the public – although it is acknowledged that additional languages would be beneficial and that routine updates are challenging given the size of the business globally, and the number of new businesses we acquire each year which need to be integrated into our compliance programme.

Data breaches have been captured and managed since 2018 using a privacy compliance tool from Onetrust (the most widely used platform to operationalise privacy, security & data governance). The business manages breaches as per the requirements of the EU General Data Protection Regulation or as per applicable local legislation.

As per the Sustainability Accounting Standards Board requirements a data breach is defined as "the unauthorised movement or disclosure of sensitive information to a party, usually outside the organisation, that is not authorised to have or see the information."

1) Number of data breaches

- There have been limited data breaches within the organisation globally. Only three incidents have been reported to regulators – two in the UK and one in Ireland. These were in relation to different breaches. No further action was taken by the regulators as the businesses satisfied the regulators that appropriate measures and mitigation had been taken
- UK reported breaches: One breach related to an office break-in where 'old' laptops without security / passwords had been stolen from the premises. The other breach was related to a system configuration incident where customer details were shared accidentally with some other customers. All impacted customers were notified and errors rectified

- Irish reported breach: This incident related to a misdirected email sent to employees internally – no customer data was involved

2) % involving customers' confidential business information

- Two out of three reported breaches involved customer data. All impacted customers were identified – less than 1,000 – they were notified and corrective action taken